psc

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB DOCKET 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date Filed: February 26, 2008

Name of company covered by this certification: Perry-Spencer RTC Inc. (d/b/a PSC) and Perry-Spencer Communications Inc. (d/b/a PSC)

Form 499 Filer ID: 805320 and 818846

Name of Signatory: James M. Dauby

Title of Signatory: President/CEO

I, James M. Dauby, certify that I am an officer of the companies named above, and acting as an agent of the companies, that I have personal knowledge that the companies have established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the companies' procedures ensure that the companies are in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The companies have not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. The companies do not have any information to report with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The companies have not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed James M. Dauby

PSC

11877 E. State Road 62 P.O. Box 126 Saint Meinrad, Indiana 47577

(812) 357-2123 Fax (812) 357-2211

www.psci.net psc@psci.net

psc

Statement of Explanation: CPNI Compliance

The operating procedures of Perry-Spencer Rural Telephone Cooperative, Inc. (d/b/a PSC) and of Perry-Spencer Communications (d/b/a PSC) are designed to ensure compliance with the CPNI rules applicable to them (including the new CPNI rules effective December 8, 2007). Such compliance procedures are as follows:

- PSC has designated a CPNI compliance officer and a backup compliance officer for the company. PSC maintains CPNI files, including the tracking of all customer complaints for one year, tracking of CPNI breaches for two years, and all Opt-Out customers. The compliance officer reviews and approves all marketing and sales campaigns and stores copies in the CPNI file. The compliance officer supervises and trains all company employees with access to CPNI.
- PSC trains and certifies all company employees with access to CPNI regarding CPNI requirements.
- PSC only shares call detail records (CDR's) by mailing the CDR to the customers' address of record (of at least 30 days) or in person after confirming the customer's identity with a valid, government-issued ID. PSC authenticates all customers to discuss any non-CDR details on their accounts.
- PSC uses an Opt-Out approach to target market products and services outside the existing customer relationship. PSC sends opt-out notices to all customers every two years. PSC also sends opt-out notices to all new customers. Opt-out status is clearly shown on the customers' accounts.
- PSC has a process in place to notify customers of account changes (address changes, etc.). PSC mails a generic letter to those customers within 48 hours regarding a change being made to their account.
- PSC will notify law enforcement (the FBI and the United States Secret Service) within seven business days after a breach occurs. After the seven days waiting period for law enforcement notification, PSC will notify the customer of any CPNI breach.
- PSC has established disciplinary procedures for employee violations of CPNI rules whether intentional or unintentional.
- PSC will take measures to discover and protect against pretexting and unauthorized disclosures of CPNI. PSC recognizes they have a 'general duty' to protect CPNI and will take measures to protect their customers' CPNI.
- PSC will file an annual certification and statement of CPNI compliance by March 1st each year.

PSC
11877 E. State Road 62 P.O. Box 126 Saint Meinrad, Indiana 47577
(812) 357-2128 Fax (812) 357-2211
www.pscinet psc@pscinet

800 RESPONSE INFORMATION SERVICES LLC

February 22, 2008

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street SW
Suite TW-A325
Washington, D.C. 20554

Re: EB Docket No. 06-36
Annual CPNI Certification for Year 2007

Dear Ms. Dortch:

Enclosed for filing pursuant to 47 CFR 64.2009(e), please find 800 Response Information Service LLC's annual CPNI certification and statement for the calendar year 2007.

Please feel free to contact me if you have any questions.

Sincerely,

Linda Young
Vice President, Operations

Enclosure

CC: Federal Communications Commission (two copies)
Enforcement Bureau
Telecommunications Consumers Division
445 12th Street, SW
Washington, D.C. 20554

Best Copy and Printing, Inc. (one copy)
445 12th Street, SW
Suite CY-B402
Washington, DC 20554

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date filed: February 22, 2008

Name of company covered by this certification: 800 Response Information Services LLC

Form 499 Filer ID:

Name of signatory: Linda Young

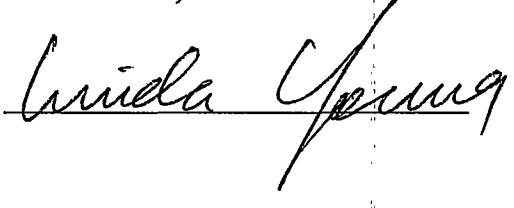
Title of signatory: Vice President of Operations

I, Linda Young, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI. If affirmative: NA.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information). If affirmative: NA

Signed 

800 Response Information Services LLC

CPNI Compliance Statement

800 Response Information Services LLC (800 Response) has the following safeguards in place to ensure that it is in compliance with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 et seq.

Compliance Officer

800 Response has appointed a CPNI Compliance Officer. The Officer is responsible for ensuring that the Company is in compliance with all CPNI rules. The Officer also communicates with the company's attorney regarding CPNI compliance matters. The Compliance Officer and/or the company's attorney is point of contact for anyone with questions about CPNI.

Employee Training

The Compliance Officer arranges for training of all employees. The training includes but is not limited to, the general safeguarding requirements for CPNI, when employees are and are not authorized to use CPNI, and the authentication methods 800 Response uses when disclosing CPNI to its customers. The detail of the training differs on whether the employee has access to CPNI.

Employees are trained that if they ever have any questions about the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer or the company's attorney immediately.

Disciplinary Process

The Company has established a disciplinary process for improper use of CPNI. Any unauthorized use, sale or other disclosure of CPNI by any employee would subject the employee to disciplinary action, up to and including dismissal.

Customer Authentication

800 Response does not disclose any CPNI to a customer based upon customer-initiated contact until the customer has been authenticated as follows:

In-Office Visit – Customers have not historically visited 800 Response's office. Should such a visit occur, the customer would be required to provide a valid photo ID matching the customer's account information

Customer-Initiated Call – All of 800 Response's customers are business customers. Accordingly, 800 Response uses the business customer exception in dealing with

customer-initiated calls. 800 Response's service contracts protect the customer's CPNI by, among other things, designating and identifying specific individuals within the customer's organization who may act on the customer's behalf. Further, 800 Response's customers have dedicated account representatives whose interactions with the customer may involve CPNI. Otherwise, 800 Response will only disclose CPNI by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide CPNI to 800 Response during a customer-initiated call without 800 Response's assistance, then 800 Response may discuss such CPNI as provided by the customer.

On-Line Access – All on-line customer access to their CPNI is password protected.

Marketing Campaigns

800 Response and its affiliates do not use customer CPNI to market its services.

If 800 Response should decide to utilize CPNI in marketing campaigns, such campaigns would be limited to the marketing of enhanced service offerings to its inter-exchange services (provided that the customer already subscribes to the inter-exchange services). Should 800 Response engage in such marketing, supervisory approval would be required for all such outbound marketing plans and records of any such marketing campaigns that utilize customers' CPNI would be maintained for a minimum of one year.

Customer Request for Approval to Use CPNI

800 Response does not sell, rent or otherwise disclose customers' CPNI to other entities. Nor does 800 Response or its affiliates use CPNI for any purpose other than to provide contracted for services to its customers. Accordingly, 800 Response does not seek either opt-in or opt-out approval to use, sell, rent or otherwise disclose a customer's CPNI.

Disclosure of CPNI to 800 Response's Affiliates

If a customer subscribes to and signs a service contract with both 800 Response and 800 Response's affiliate for inter-exchange services which are provided by 800 Response and related enhanced services to the inter-exchange services which are provided by such affiliate, 800 Response discloses such customer's CPNI to the affiliate for the purpose of providing such contracted for services to the customer.

Disclosure of CPNI to Customer's Agent at Customer's Request

When specifically requested in writing and signed by an authorized representative of a customer, 800 Response provides such customer's CPNI to an authorized agent of the customer, all as directed by the customer.

Security Breach of CPNI

The requirements under 47 C.F.R. § 64.2011 *Notification of customer proprietary network information security breaches* will be followed should a breach of its customers' CPNI occur. No breach occurred in 2007.

Customer Complaints Regarding CPNI

No customer complaints regarding the unauthorized release of CPNI were received in 2007